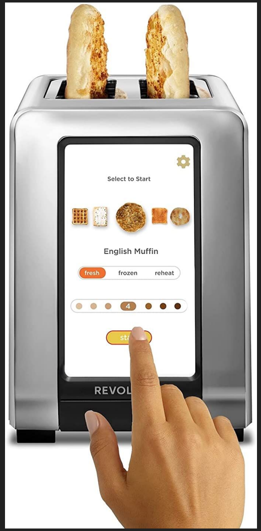
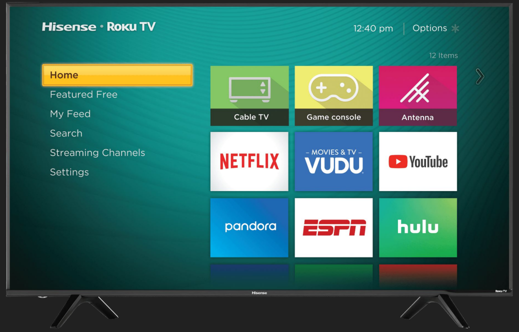
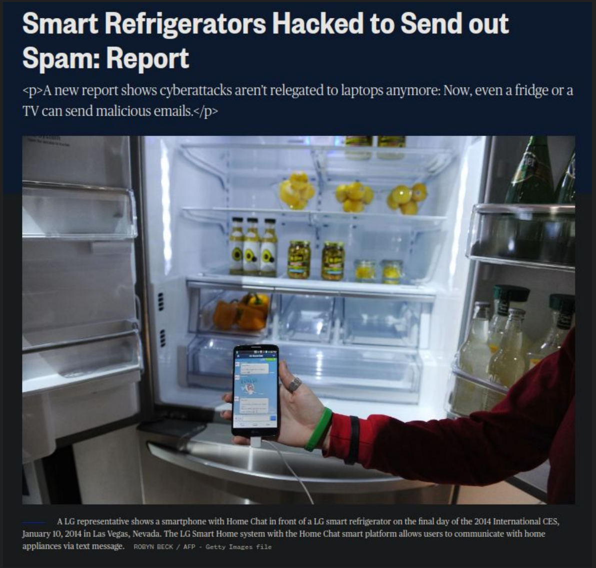
IoT-Hacking

The “S” is for security ;)


Select to Start
English Muffin
fresh
frozen
reheat
4
REVOL

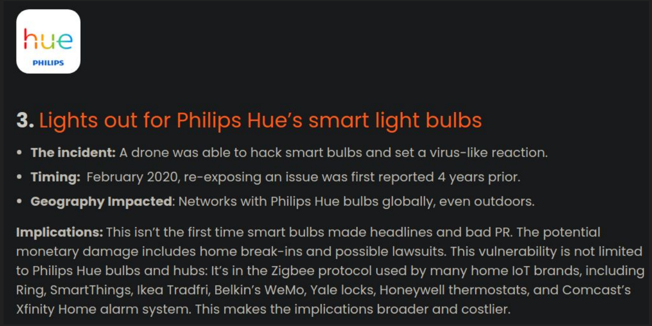

Hisense · Roku TV
12:40 pm
Options
12 Items
Home
Featured Free
My Feed
Search
Streaming Channels
Settings
Cable TV
Game console
Antenna
NETFLIX
MOVIES & TV
VUDU
YouTube
pandora
ESPN
hulu



Smart Refrigerators Hacked to Send out Spam: Report

<p>A new report shows cyberattacks aren't relegated to laptops anymore: Now, even a fridge or a TV can send malicious emails.</p>

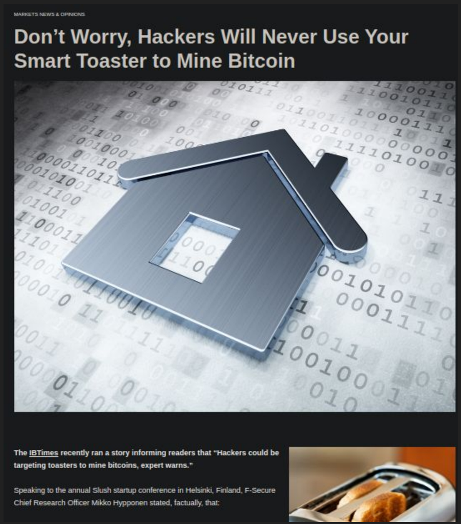
A LG representative shows a smartphone with Home Chat in front of a LG smart refrigerator on the final day of the 2014 International CES, January 10, 2014 in Las Vegas, Nevada. The LG Smart Home system with the Home Chat smart platform allows users to communicate with home appliances via text message. ROBYN BECK / AFP - Getty Images file



3. Lights out for Philips Hue's smart light bulbs

- **The incident:** A drone was able to hack smart bulbs and set a virus-like reaction.
- **Timing:** February 2020, re-exposing an issue was first reported 4 years prior.
- **Geography Impacted**: Networks with Philips Hue bulbs globally, even outdoors.

Implications: This isn't the first time smart bulbs made headlines and bad PR. The potential monetary damage includes home break-ins and possible lawsuits. This vulnerability is not limited to Philips Hue bulbs and hubs: It's in the Zigbee protocol used by many home IoT brands, including Ring, SmartThings, Ikea Tradfri, Belkin's WeMo, Yale locks, Honeywell thermostats, and Comcast's Xfinity Home alarm system. This makes the implications broader and costlier.

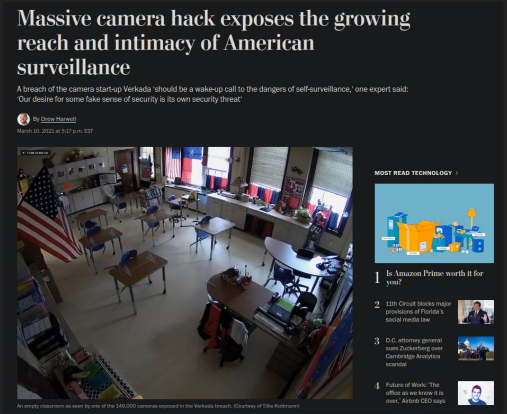


MARKETS NEWS & OPINIONS

Don't Worry, Hackers Will Never Use Your Smart Toaster to Mine Bitcoin

The IBTimes recently ran a story informing readers that "Hackers could be targeting toasters to mine bitcoins, expert warns."

Speaking to the annual Slush startup conference in Helsinki, Finland, F-Secure Chief Research Officer Mikko Hypponen stated, factually, that:



Massive camera hack exposes the growing reach and intimacy of American surveillance

A breach of the camera start-up Verkada 'should be a wake-up call to the dangers of self-surveillance,' one expert said: 'Our desire for some fake sense of security is its own security threat'

By Drew Harwell

March 10, 2021 at 5:17 p.m. EST

An empty classroom as seen by one of the 149,000 cameras exposed in the Verkada breach. (Courtesy of Tillie Kottmann)

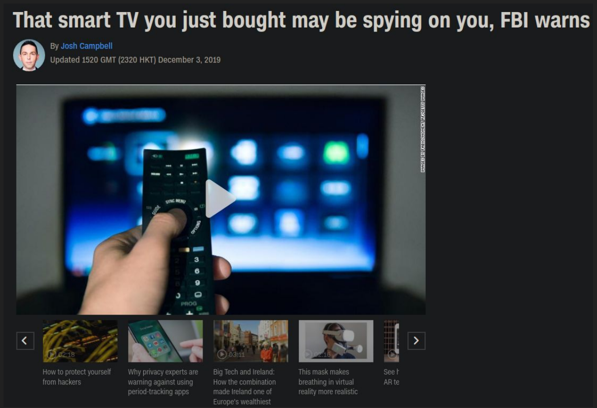
MOST READ TECHNOLOGY ›

1 Is Amazon Prime worth it for you?

2 11th Circuit blocks major provisions of Florida's social media law

3 D.C. attorney general sues Zuckerberg over Cambridge Analytica scandal

4 Future of Work: 'The office as we know it is over,' Airbnb CEO says



That smart TV you just bought may be spying on you, FBI warns

By Josh Campbell

Updated 1520 GMT (2320 HKT) December 3, 2019

How to protect yourself from hackers

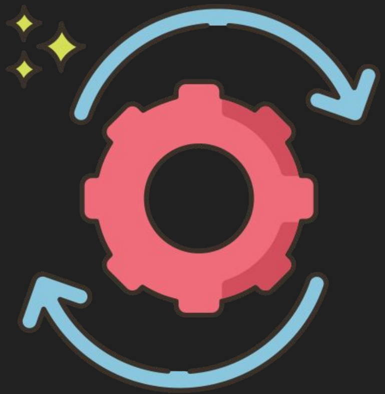
Why privacy experts are warning against using period-tracking apps

Big Tech and Ireland: How the combination made Ireland one of Europe's wealthiest

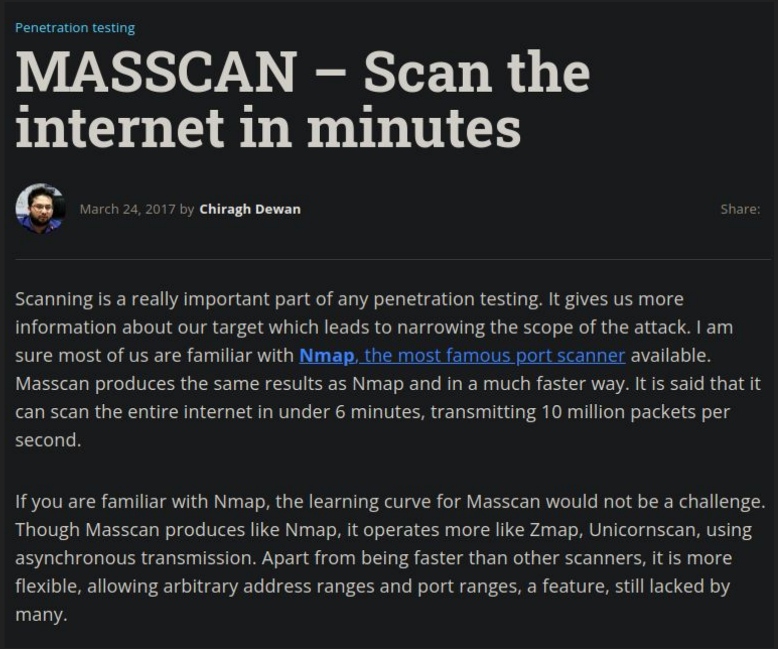
This mask makes breathing in virtual reality more realistic

See h AR te

Why is IoT missing the “S”?



How?



Penetration testing

MASSCAN – Scan the internet in minutes

March 24, 2017 by **Chiragh Dewan**

Share:

Scanning is a really important part of any penetration testing. It gives us more information about our target which leads to narrowing the scope of the attack. I am sure most of us are familiar with **Nmap**, the most famous port scanner available. Masscan produces the same results as Nmap and in a much faster way. It is said that it can scan the entire internet in under 6 minutes, transmitting 10 million packets per second.

If you are familiar with Nmap, the learning curve for Masscan would not be a challenge. Though Masscan produces like Nmap, it operates more like Zmap, Unicornscan, using asynchronous transmission. Apart from being faster than other scanners, it is more flexible, allowing arbitrary address ranges and port ranges, a feature, still lacked by many.

Default Passwords: The Biggest Weakness in IoT Security

06
FEB 2018

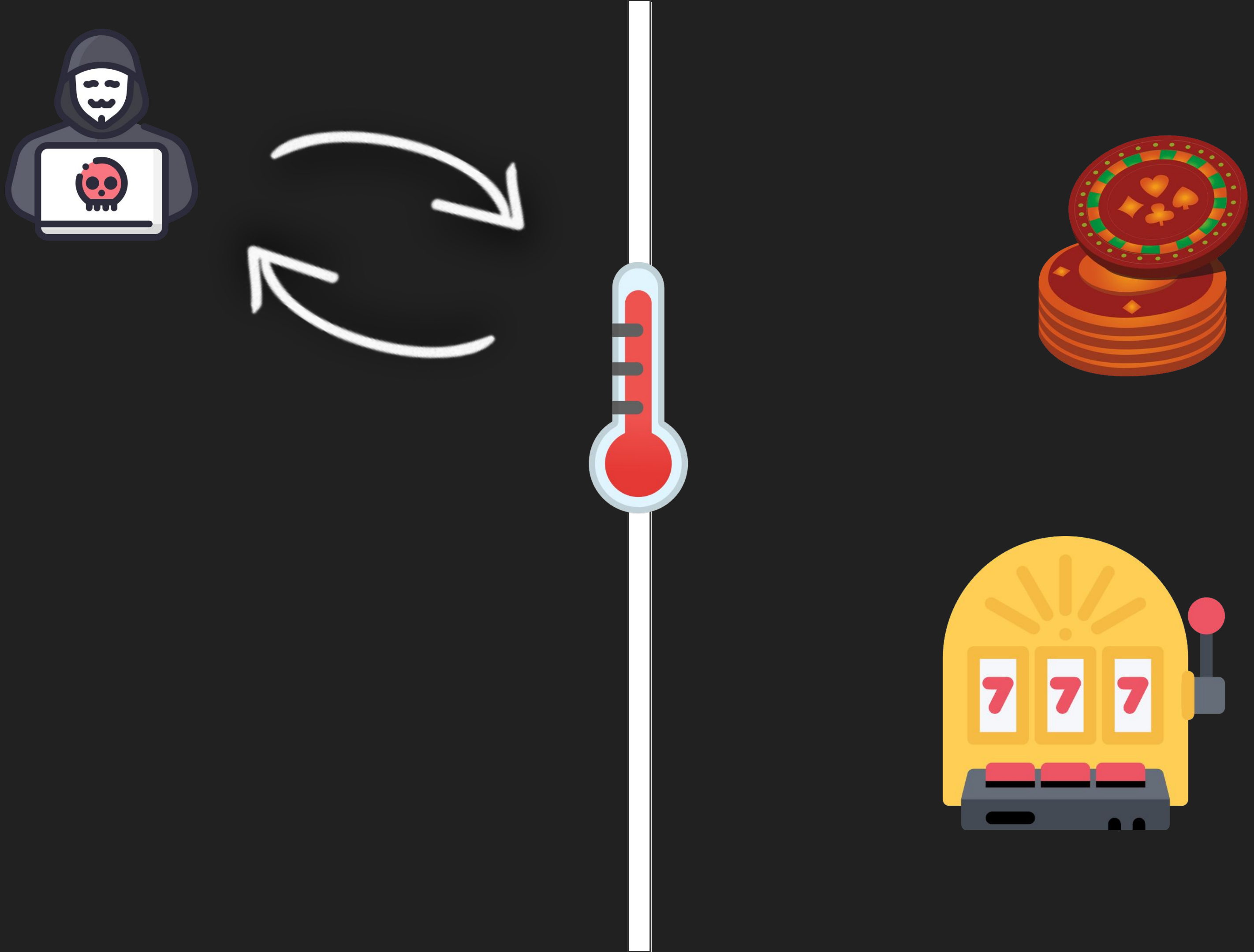
IOT, Password Security, Security, Security Threats   IoT, password security, security, security threats   Ophtek, LLC

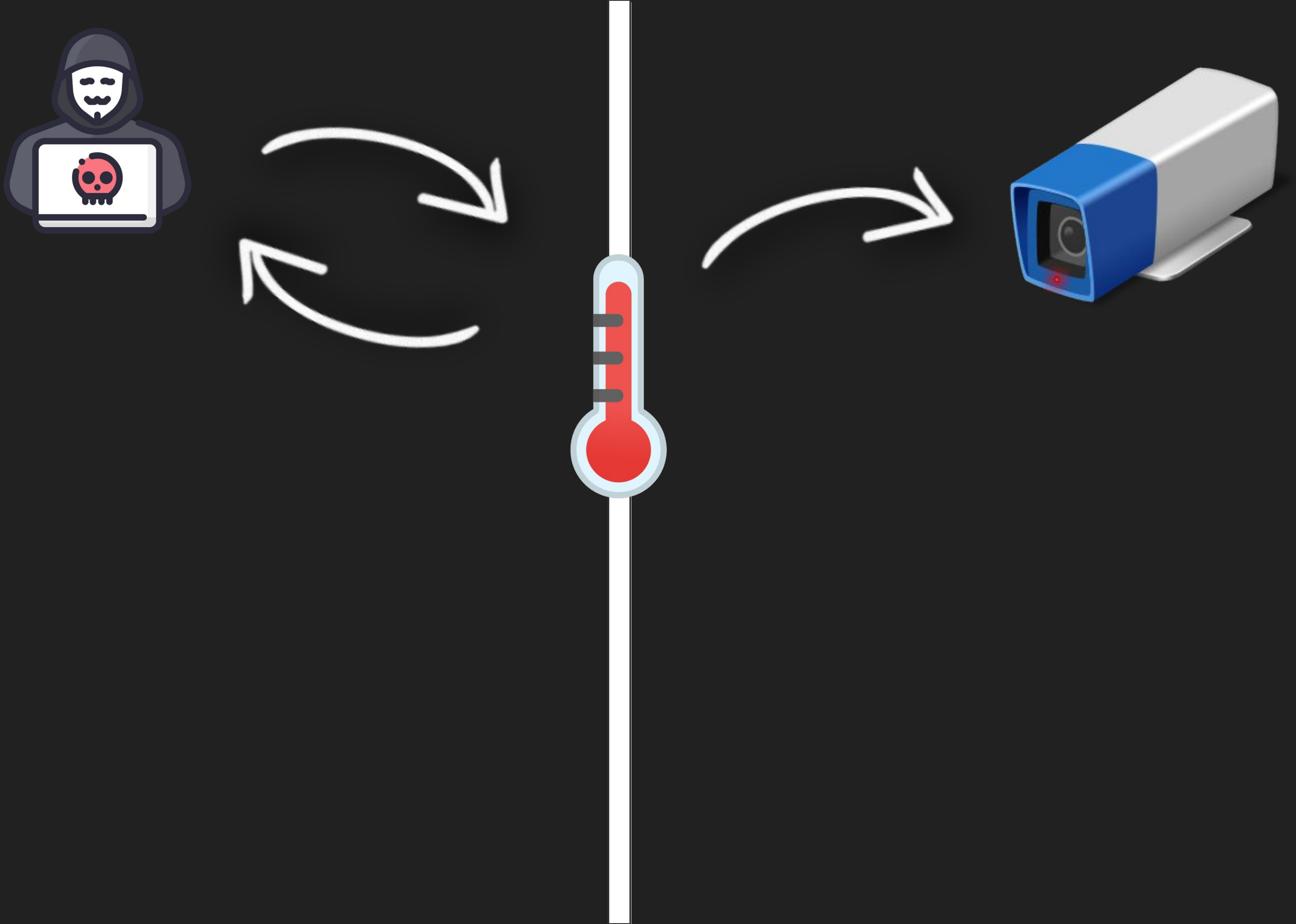
The Heist

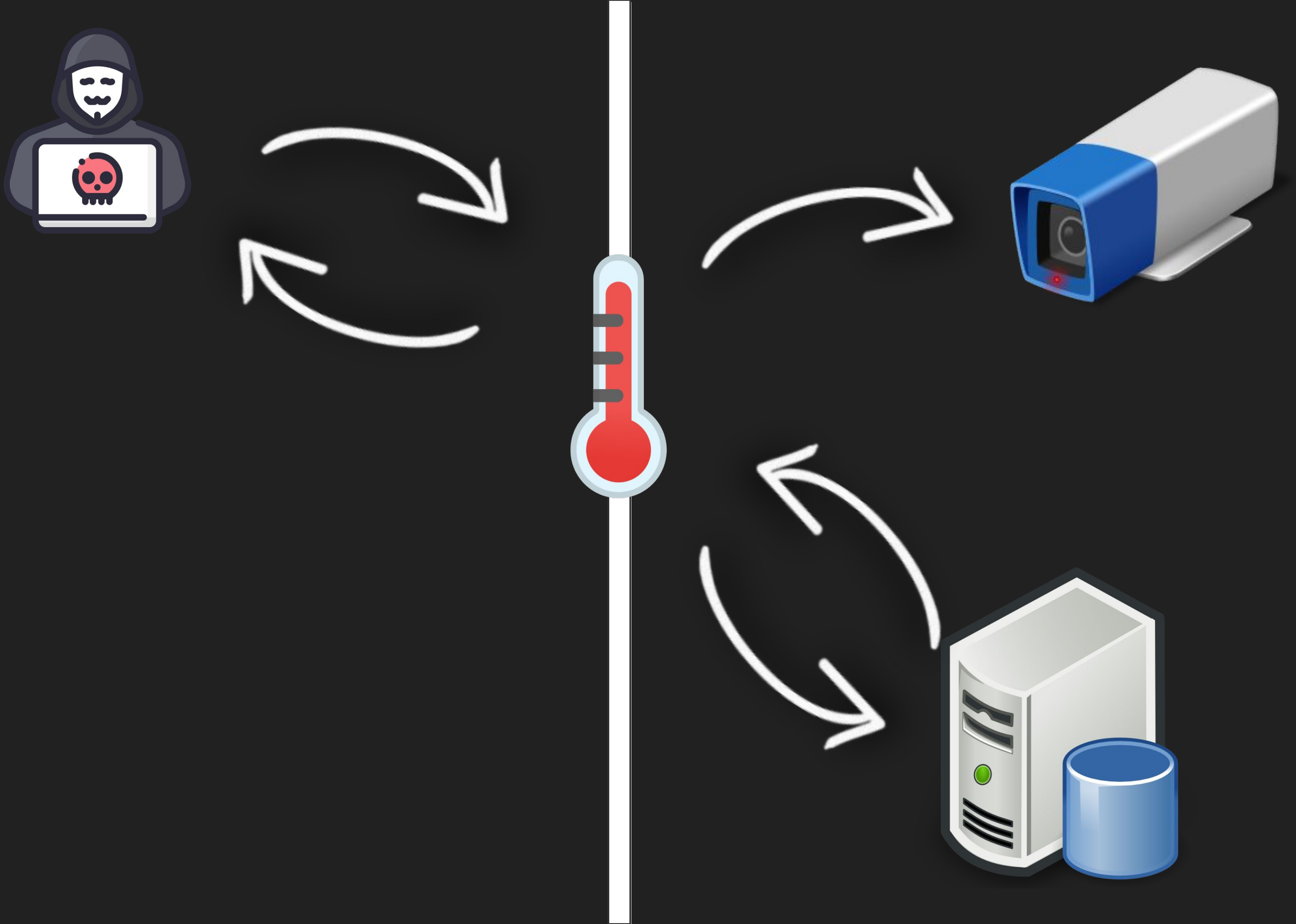
7
7
7

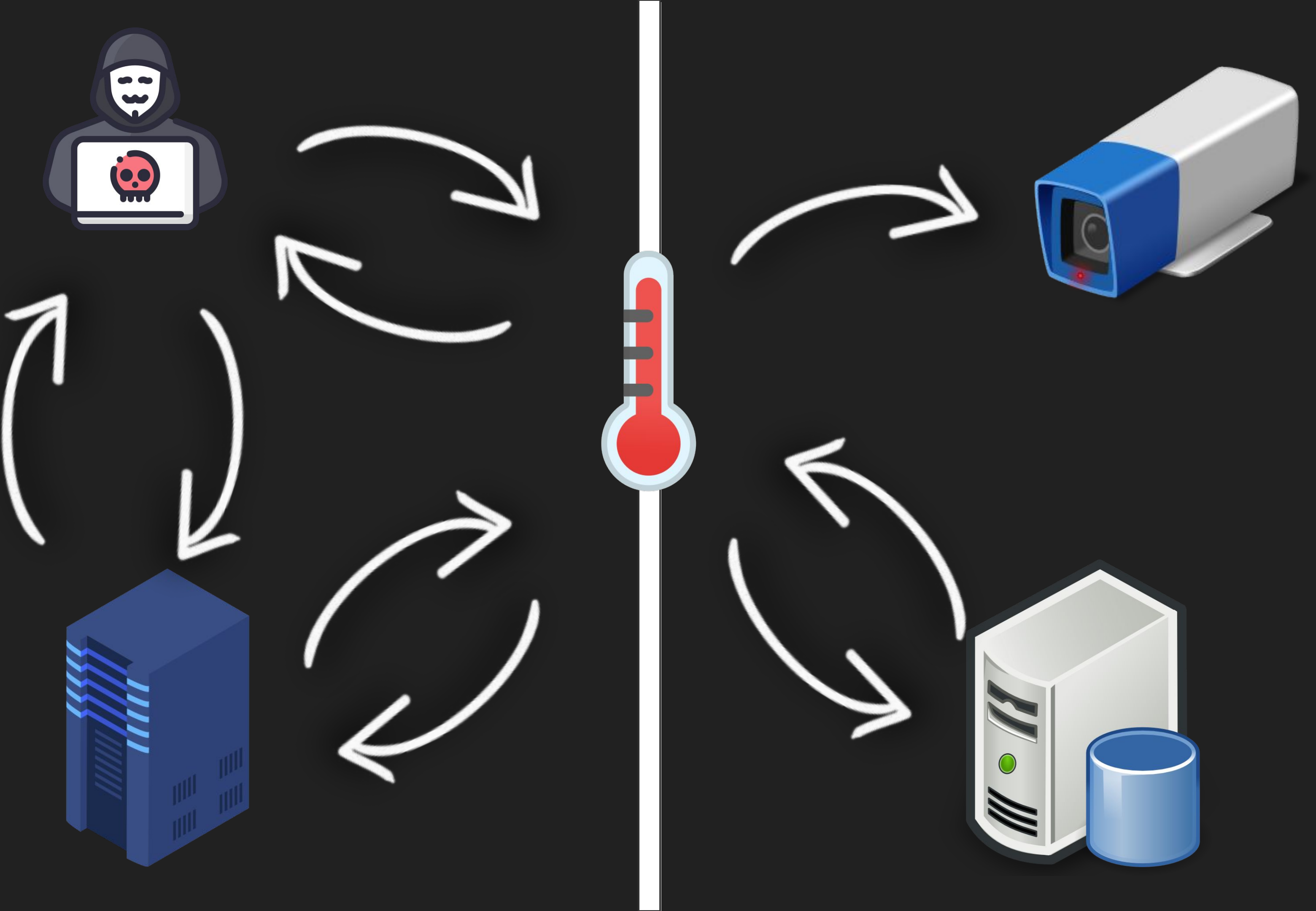
DRINK

7 7 7


7 7 7







Let’s hack

https://github.com/Pengrey/IoT-Hacking